

RANDOM NUMBER GENERATOR

Patent Number: JP7134647
 Publication date: 1995-05-23
 Inventor(s): KATSUTA NOBORU; others: 03
 Applicant(s): MATSUSHITA ELECTRIC IND CO LTD
 Requested Patent: ☐ JP7134647
 Application Number: JP19930279529 19931109
 Priority Number(s):
 IPC Classification: G06F7/58; G09C1/00
 EC Classification:
 Equivalents:

Abstract

PURPOSE: To provide a random number generator for simultaneously outputting plural random number sequences by utilizing parts whose phases are sufficiently separated from each other in one random number sequence related to the random number generator for generating pseudo random sequences.
CONSTITUTION: An M sequence is generated by flip-flop circuits 1 to 31, AND circuits 61 and 62 and exclusive OR circuits 42 and 43 and output of the flip-flop circuits 10 to 19 at this time is taken out as the output. Then, the output is calculated in the exclusive OR circuits 44 to 60 and thus, random number sequences are found in which the adjacent random numbers are shifted by 262142 shift clocks from each other and further, a random number ratio is controlled by the ratio of '1' and '0' in rate signals and the output is attained.

Data supplied from the esp@cenet database - I2

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平7-134647

(43)公開日 平成7年(1995)5月23日

(51)Int.Cl.⁵

識別記号

庁内整理番号

F I

技術表示箇所

G 0 6 F 7/58

C

G 0 9 C 1/00

9364-5L

審査請求 未請求 請求項の数 4 O L (全 5 頁)

(21)出願番号

特願平5-279529

(22)出願日

平成5年(1993)11月9日

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 勝田 昇

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 村上 弘規

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 茨木 晋

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74)代理人 弁理士 小鍛冶 明 (外2名)

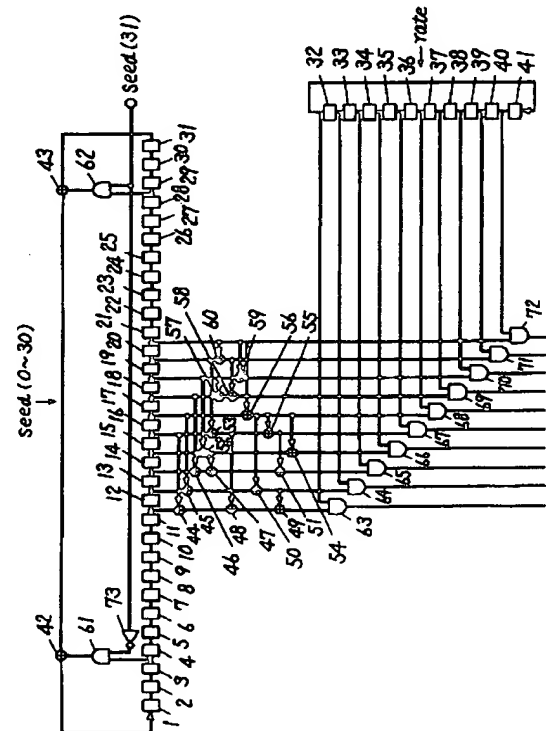
最終頁に続く

(54)【発明の名称】 乱数発生装置

(57)【要約】

【目的】 本発明は、疑似ランダム系列を生成する乱数発生装置に関するもので、1つの乱数列中の十分位相の離れた部分を利用して複数の乱数列を同時に出力する乱数発生装置を提供することを目的とする。

【構成】 フリップフロップ回路1から31、論理積回路61および62、排他的論理和回路42および43でM系列を生成し、このときのフリップフロップ回路10から19の出力を出力として取り出し、次に、これらの出力を排他的論理和回路44から60で演算することで隣同士が262142シフトクロックずれた乱数列にし、さらにrate信号中の1と0の比率で乱数比を制御し出力とする。



【特許請求の範囲】

【請求項 1】 ビットを記憶する複数の記憶手段と各記憶手段が記憶する信号をそれぞれ隣接する記憶手段にシフトさせるとともに記憶手段に記憶されたビット値の線形結合した値をフィードバックするシフトおよびフィードバック手段からなる M 系列乱数発生手段と、少なくとも 1 つ以上の排他的論理和演算手段とを具備し、各排他的論理和手段は、前記 M 系列乱数発生手段中の複数の記憶手段の出力の排他的論理和結合を演算する排他的論理和手段であり、前記 M 系列乱数発生手段中の記憶手段の出力もしくは排他的論理和手段の出力からなる複数の乱数出力をもつことを特徴とする乱数発生装置。

【請求項 2】 M 系列乱数発生手段中のフィードバック手段は、そのフィードバック方法を示した原始多項式が、互いに相反多項式となる 2 通りのフィードバック手段をもち、制御信号によって 2 つのフィードバック手段のどちらか一方を選択する選択手段を具備したことを特徴とする請求項 1 記載の乱数発生装置。

【請求項 3】 乱数発生手段と複数のビットを記憶する記憶手段と論理積回路を具備し、前記記憶手段は、前記乱数発生手段の出力同期して記憶している信号を 1 巡回シフトし、前記論理積回路は、乱数発生装置のそれぞれの出力と記憶手段のビット出力との論理積を出力することを特徴とする乱数発生装置。

【請求項 4】 M 系列乱数発生手段中のフィードバック手段は、そのフィードバック方法を示した原始多項式が、互いに相反多項式となる 2 通りのフィードバック手段をもち、制御信号によって 2 つのフィードバック手段のどちらか一方を選択する選択手段を具備したことを特徴とする請求項 3 記載の乱数発生装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、デジタルデータをランダム化する際にデータに加算する乱数を発生させる乱数発生器に関するもので、一度に複数のビットの乱数列を生成する乱数発生装置に関するものである。

【0002】

【従来の技術】 従来の乱数発生装置としては、例えば暗号と情報セキュリティ（昭晃堂）pp158に示されているような線形フィードバックレジスタによるものがある。図 2 は、この従来の乱数発生装置の構成図を示すものである。図 2 において、74 はクロックパルスが入力される毎に入力されている値を保持する n 個の記憶回路からなる記憶回路群、75 は排他的論理和回路群、76 は接続か接続しないかを制御するスイッチ群である。

【0003】 以上のように構成された従来の乱数発生装置においては、まず、記憶回路群 74 へ初期値が入力される。次に、乱数を取り出す毎にクロックパルスが入力される。そのとき記憶回路群 74 中のそれぞれの記憶回路に記憶されている値は、右隣の記憶レジスタにシフト

され記憶されるとともに、一番左にある記憶回路へは、各記憶回路の出力の線形結合演算結果がフィードバックされる。この際、フィードバックのしかたを示す特性多項式を

$$h(x) = 1 - h_1 x - h_2 x^2 - \dots - h_n x^n$$
 (h_i は、0 または 1 で接続または非接続)

としたとき、 $h(x)$ が原始多項式で表現される場合、各レジスタに記憶される値の時系列みた場合の乱数系列は、M 系列の乱数列を生成される。この M 系列は、乱数としての特性もよく一般に広く用いられている。

【0004】

【発明が解決しようとする課題】 しかしながら前記のような従来の構成では、乱数値は、1 クロックパルス毎に 1 ビットしか乱数が新たに発生しない。スクランブル効果制御などデータ中の特定の符号にのみ乱数を加算したいときなどは、その符号を検出して処理するなど 1 ビット単位で処理するよりも複数のビットからなる符号単位でその符号中の複数のビットを同時に処理したい場合がある。このような複数ビットの出力が必要な場合においては、従来例のような乱数発生装置では、用いるビット数だけクロックパルスを生成する必要があり、乱数発生装置が接続されている装置のクロックに比べて、同時に必要なビット数倍だけ高速なクロックが乱数発生装置に必要な問題があった。

【0005】 これを解決する手段として、乱数発生装置を複数個用意することが考えられるが、回路規模が大きくなる問題があり、また、各レジスタの出力を用いた場合には、各レジスタの出力の系列は、単にレジスタ間のシフト数分だけずれているだけであり、同じ乱数列を使うことになり、データ中の同じ乱数が加算されているデータ同士を加算しあうことで、乱数の影響を取り除くことができる問題があった。

【0006】 本発明はかかる点に鑑み、一つの乱数発生装置で複数の出力をもち、そのそれぞれから出力される乱数列がそれぞれ独立な乱数として利用可能な乱数発生装置を提供することを目的とする。

【0007】

【課題を解決するための手段】 第 1 の発明は、ビットを記憶する複数の記憶手段と各記憶手段が記憶する信号をそれぞれ隣接する記憶手段にシフトさせるとともに記憶手段に記憶されたビット値の線形結合した値をフィードバックするシフトおよびフィードバック手段からなる M 系列乱数発生手段と少なくとも 1 つ以上の排他的論理和演算手段を具備し、各排他的論理和手段は、前記 M 系列乱数発生手段中の複数の記憶手段の出力の排他的論理和結合を演算する排他的論理和手段であり、前記 M 系列乱数発生手段中の記憶手段の出力もしくは排他的論理和手段の出力からなる複数の乱数出力をもつ構成である。

【0008】 また、第 2 の発明は、乱数発生手段と複数のビットを記憶する記憶手段と論理積回路を具備し、記憶

手段は、乱数発生手段の出力と同期して記憶している信号を 1 巡回シフトし、論理積回路は、乱数発生装置のそれぞれの出力と記憶手段のビット出力との論理積を出力する構成である。

【 0 0 0 9 】

【作用】第 1 の発明は前記した構成により、乱数発生装置の出力は、数シフト分ずれた同じ M 系列を排他的論理和演算したことになる。同じ M 系列で a だけずれたもの同士の排他的論理和して生成される系列は、同じ M 系列の乱数列となり、最初の乱数列の位置からのずれ b は、

$$x^b = 1 + x^a \pmod{h(x)}$$

によって決定される。これより b は、 $h(x)$ の次数以上の値となり、その時点で M 系列乱数発生手段中に保持されている値より離れたシフト数の位置の乱数列を生成できる。

【 0 0 1 0 】したがって、排他的論理和演算を組み合わせることによって、各出力を 1 つの M 系列の乱数列中のそれぞれ十分離れた位置から切り出し出力できるので、各出力の乱数列中の位相差より使用するビット数が少ない範囲内で、それぞれ別々の乱数列とみなし、利用できる。また、さらに、フィードバックの仕方を互いに相反多項式になる原始多項式の間で切り換えてやると、同じ系列を全く逆の順番に出力するようになるため、各出力の位相関係を保持したまま、フィードバックの切り換えによって複雑な乱数列を生成でき、乱数を暗号化に用いた場合の安全を向上できる。

【 0 0 1 1 】また、第 2 の発明は前記した構成により、乱数発生装置の出力部に、記憶手段に入力された信号を巡回シフトしながらデータが論理積演算されるので、乱数中の 1 と 0 の比率が、記憶手段に入力される信号の 0 と 1 の比率によって制御できるとともに、線形処理でない論理積演算が加わることで、暗号に用いた場合の安全性も向上する。

【 0 0 1 2 】

【実施例】以下、本発明の第 1 の実施例について、図面を参照しながら説明する。図 1 は本発明の第 1 の実施例における乱数発生装置の構成図を示すものである。

【 0 0 1 3 】図 1 において、1 から 4 1 はフリップフロップ回路で、共通のシフトクロックパルス信号が入力できるように配線が施されており、4 2 から 6 0 は排他的論理和回路、6 1 から 7 2 は論理積回路、7 3 は反転回路である。

【 0 0 1 4 】以上のように構成されたこの実施例の乱数発生装置において、以下その動作を説明する。最初に、乱数発生装置を所望の値で初期化して動作させる。これは、3 2 ビットの seed と 1 0 ビットの rate 信号であり、seed の下位 3 1 ビットをフリップフロップ回路 1 から 3 1 にセットし、seed の上位 1 ビットを論理積回路 6 1 および 6 2 の入力信号としてセットし、rate 信号をフリップフロップ回路 3 2 から 4 1 にセットする。

【 0 0 1 5 】フリップフロップ回路 1 から 3 1、論理積回路 6 1 および 6 2、排他的論理和回路 4 2 および 4 3 で M 系列を生成する乱数発生手段となっており、seed の最上位ビットが 1 のとき論理積回路 6 2 の出力がオン状態となり、原始多項式 $1 - x^{2^3} - x^{3^1}$ で生成される M 系列を生成し、seed の最上位ビットが 0 のとき論理積回路 6 1 の出力がオン状態となり、原始多項式 $1 - x^3 - x^{3^1}$ で生成される M 系列の乱数列をシフトクロックパルス毎に生成する。原始多項式 $1 - x^{2^3} - x^{3^1}$ と原始多項式 $1 - x^3 - x^{3^1}$ は、互いに相手の相反多項式であるので、お互いの乱数を逆の順序で発生する関係にある。そして、このときのフリップフロップ回路 1 1 から 2 0 の出力を M 系列乱数発生手段の出力として取り出す。これらの乱数列は、フリップフロップ回路 1 1 の信号を先頭に順に 1 シフトずつ遅れた同じ乱数列となっている。

【 0 0 1 6 】次に、これらの出力を排他的論理和回路 4 4 から 6 0 で演算することで隣同士が 2 6 2 1 4 2 シフトクロックずれた乱数列にしている。これは、例えば以下のように設定している。フリップフロップ 2 0 は、隣のフリップフロップ 1 9 の出力に排他的論理和演算すると 2 6 2 1 4 2 シフトクロック分フリップフロップ 2 0 の出力より遅れたもしくは進んだ信号となる。するとフリップフロップ 2 0 の出力とフリップフロップ 1 8 の排他的論理和は、2 6 2 1 4 2 シフトクロック遅れたもしくは進んだフリップフロップ 2 0 と 1 9 の出力の排他的論理和とそれよりさらに 1 シフト遅れたもしくは進んだフリップフロップ 1 9 と 1 8 の排他的論理和の 2 つを排他的論理和したものと同値となり、2 倍の 5 2 4 2 8 4 シフトクロック遅れたもしくは進んだ信号が生成される。以下も同様な手法で排他的論理和演算を組み合わせ、所定のシフト数遅らせるもしくは進ませるている。

【 0 0 1 7 】次に、rate 信号による処理を説明すると、フリップフロップ回路 3 2 から 4 1 にセットされた信号は、シフトクロック毎に 1 巡回シフトしたことになる。そして、それぞれのフリップフロップの出力は、乱数発生手段の出力と論理積演算される。したがって、出力 r_n から r_{n+9} は、rate 信号の 1 0 ビットパターンの中の 1 が立っているところのみ、M 系列の乱数を出力し、0 の時は、そのまま 0 の状態となるので、rate 信号中の 0 と 1 の比を t とすると出力 r_n から r_{n+9} 中の 1 と 0 の比は、 $t \times 1/2$ となり、rate 信号によって乱数比を制御し出力とする。

【 0 0 1 8 】以上のようにこの実施例によれば、seed の最上位ビットと論理積回路 6 1 および 6 2 を設けることにより、乱数発生手段のフィードバック位置を簡単に制御できるとともに、出力 r_n から r_{n+9} は、等シフトクロック分遅れた信号に設定しているので、seed の最上位ビットを切り換えた際にも、隣接した出力間の関係は、全く対象になっており、1 つの M 系列乱数中で隣同士で重なった位置を使わないで利用できる使用シフト数

が変化しないで用いることができる。

【0019】なお、本実施例においては、31ビットのシフトレジスタで構成されるM系列を用いたが、他のM系列を生成するものでもよい。また、出力の数も、必要な数を出力すればよく、出力間同士の位相差も使用するシフト数を考慮して必要十分なシフト数分だけ離してやればよいし、等間隔にする必要もない。

【0020】また、rate信号用のフリップフロップの数は、本実施例では、出力と同数にしたが、それよりも多くしてその一部を論理積回路に接続してもよいし、数が少ない場合には、複数の論理積回路に接続するしてもよい。

【0021】

【発明の効果】以上説明したように、本発明によれば、

1つの乱数系列を数シフト間隔離れた位置ごとに分割して利用することにより、1つの乱数系列発生手段で同時に複数の乱数系列を出力することができ、その実用的効果は大きい。

【図面の簡単な説明】

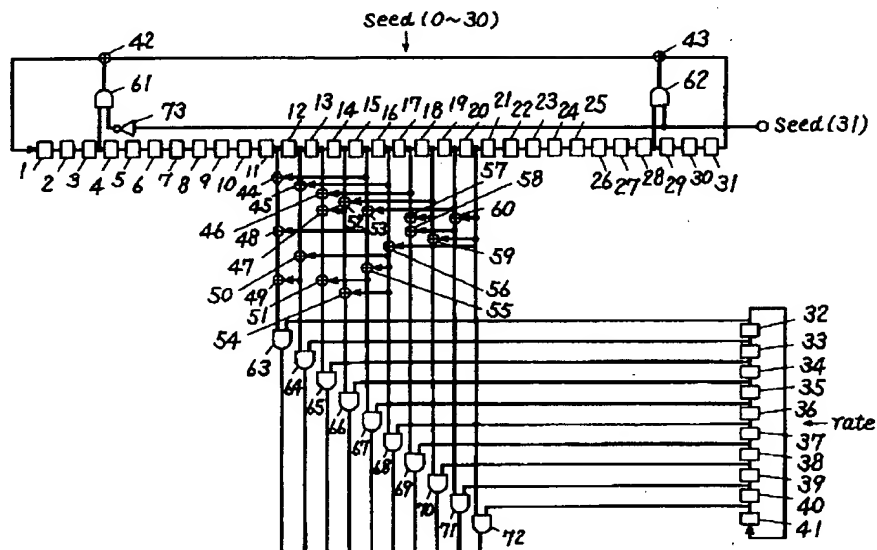
【図1】本発明の第1の実施例における乱数発生装置の構成図

【図2】従来の乱数発生装置の構成図

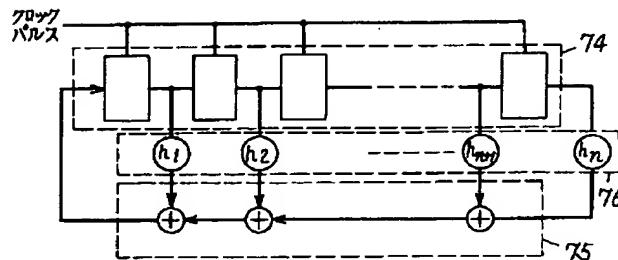
【符号の説明】

- 1～41 フリップフロップ回路
- 42～60 排他的論理和回路
- 61～72 論理積回路
- 73 反転回路

【図1】



【図2】



フロントページの続き

(72)発明者 中村 誠司
大阪府門真市大字門真1006番地 松下電器
産業株式会社内